MEDIAS ES N-05D
（Android 4.0）
VPN 接続 取扱説明書

Ver. 1.00

ＮＥＣカシオモバイルコミュニケーションズ

本書の記載について

- **本書で掲載している画面はイメージであるため、実際の画面とは異なる場合があります。また、設定の変更によって** FOMA **端末の表示・操作が本書での記載と異なる場合があります。**
- **本書の内容の一部、または全部を無断転載することは、禁止されています。**
- **本書の内容に関しては、将来予告なしに変更することがあります。**
- **本書では、**2012 **年** 10 **月** 16 **日公開の** MEDIAS ES N-05D **更新ソフトウェア**（Android4.0）**の適用を** “ **バージョンアップ** ” **と記載しています。**

1. はじめに

1.1. 本書について

本取扱説明書は、MEDIAS ES N-05D のバージョンアップ後の VPN 表示・操作について記載しています。バージョンアップ前に VPN 機能を使用されていたお客様は、本書に従い VPN の設定を再度行っていただけますようお願いいたします。

1.2. ご注意

バージョンアップに伴いご利用ができなくなる認証方式と証明書形式がございますので、現在ご利用頂いている認証方式と証明書形式が利用できるかどうかご確認の上、バージョンアップを実施頂けます様お願いいたします。詳細につきましては、「2.バージョンアップ前のご確認」を参照ください。

2. バージョンアップ前のご確認

2.1. 事前にご確認いただきたい事項、準備

バージョンアップの前後では、サポートする接続方式・証明書が異なる場合がございます。現在ご利用になっている接続方式・証明書が、バージョンアップ後に使用不可となる場合は、サーバーの設定を見直すか、バージョンアップを適用しない等のご判断をお願いいたします。

バージョンアップの前後では、VPN *の設定内容・証明書は引継がれません*。このため、VPN の設定内容・証明書を事前に控えておくなど、バージョンアップの前に準備をお願いいたします。

2.2. バージョンアップ前後の違い

2.2.1. 接続方式について

バージョンアップ後は、以下の接続方式をサポートします。

- PPTP(Point to Point Tunneling Protocol)
- L2TP/IPSecPSK（Layer 2 Tunneling Protocol / IP Security with Pre-shared key）
- L2TP/IPSecRSA（Layer 2 Tunneling Protocol / IP Security with RSA）
- IPSec Xauth PSK（IP Security eXtended AUTHentication with Pre-shared key）
- IPSec Xauth RSA（IP Security eXtended AUTHentication with RSA）
- IPSec Hybrid RSA（IP Security Hybrid with RSA）

バージョンアップ前後の接続方式名称の違い、サポート状況については下記の表を参照ください。

バージョンアップ前の接続方式名	バージョンアップ後の接続方式名
PPTP	PPTP
CRT IKEv1	－（未サポート）
CRT IKEv1(Aggr)	－（未サポート）
CRT IKEv1(Xauth)	IPsec Xauth RSA
CRT IKEv1(Xauth, Aggr)	－（未サポート）
CRT IKEv1(Xauth, Aggr, PFS)	－（未サポート）
CRT IKEv1(Xauth, PFS)	－（未サポート）
CRT IKEv2	－（未サポート）
CRT IKEv2 MOBIKE	－（未サポート）
L2TP CRT IKEv1	L2TP/IPec RSA
PSK IKEv1	－（未サポート）
PSK IKEv1(Aggr)	－（未サポート）
PSK IKEv1(Xauth)	IPsec Xauth PSK
PSK IKEv1(Xauth, Aggr)	IPsec Xauth PSK　※設定にて IPsecID を指定することで Aggr となります。
PSK IKEv1(Xauth, Aggr, PFS)	－（未サポート）

PSK IKEv1(Xauth, PFS)	―（未サポート）
PSK IKEv2	―（未サポート）
PSK IKEv2 MOBIKE	―（未サポート）
L2TP PSK IKEv1	L2TP/IPsec PSK
―（未サポート）	IPsec Hybrid RSA

2.2.2. 証明書について

証明書について、バージョンアップ前後で下記のサポートとなります。

証明書の形式	ファイル拡張子	バージョンアップ前	バージョンアップ後
X.509 DER 形式	ca	○	×
	crt	○	○
	cer	×	○
X.509 PEM 形式	ca	○	×
	crt	○	×
PKCS#12 形式	p12	○	○
	pfx	×	○

○：サポート、×：未サポート

バージョンアップ前にインストールされていた証明書は、バージョンアップ後には*引継がれません*。バージョンアップ後に、再度インポートを行ってください。証明書のインポートについては「3.3 証明書のインポート」を参照ください。

2.2.3. 設定値について

設定値について、バージョンアップ前後で下記の名称となります。

■PPTP

バージョンアップ前	バージョンアップ後
VPN 名	名前
（メニューとして選択）	タイプ（PPTP）
VPN サーバーの設定	サーバーアドレス
暗号化を有効にする	PPP 暗号化（MPPE）
DNS 検索ドメイン	DNS 検索ドメイン
―	DNS サーバー（※新規）
―	転送ルート（※新規）

■PPTP 以外の設定値

バージョンアップ前	バージョンアップ後
接続名	名前
接続テンプレート	タイプ
ゲートウェイアドレス	サーバーアドレス
証明書	IPsec ユーザー証明書
CA(認証局)証明書	IPsec CA 証明書
―	IPsec サーバー証明書（※新規）
事前共有鍵タイプ	IPSec 事前共有鍵
事前共有鍵	
識別タイプ	IPSec ID
ID	
ユーザー名	ユーザー名
パスワード	パスワード
―	DNS 検索ドメイン（※新規）
―	DNS サーバー（※新規）
内部サブネット IP	転送ルート

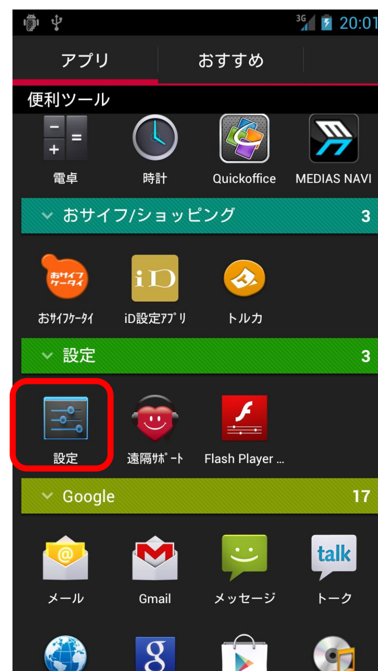
3. VPN の接続準備

VPN へ接続するための詳細設定を行います。

3.1. VPN 設定画面の起動方法

3.1.1. アプリ画面で「設定」

「設定」をタップし、設定画面を表示します。



3.1.2. 設定画面で「その他」

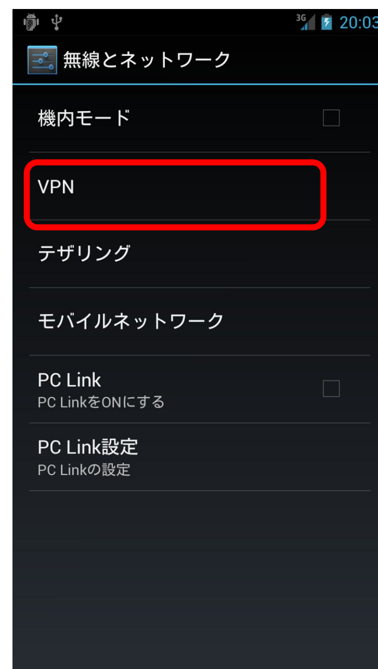
「その他」をタップし、無線とネットワークの設定画面を表示します。



3.1.3. 無線とネットワークの設定画面で「VPN」

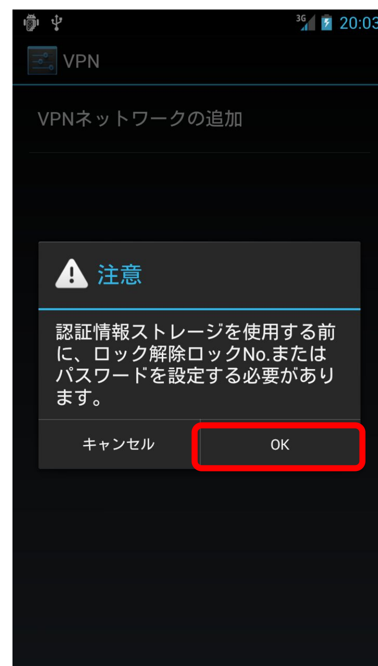
「VPN」をタップします。

初回起動時は、3.1.4 の認証設定の確認画面が表示され、2 回目以降は、エラー! *参照元が見つかりません。*の VPN 画面が表示されます。



3.1.4. 認証設定の確認画面で「OK」

「OK」をタップし、ロック解除方法の選択画面を表示します。



3.1.5. ロック解除方法の選択画面で選択

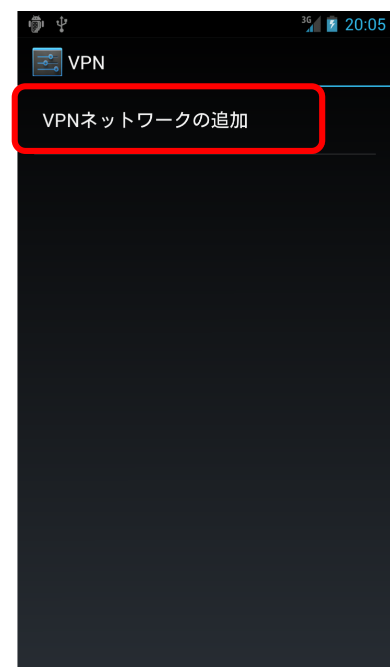
「パターン」「ロック No.」「パスワード」のいずれかを選択し設定します。



- パターン…パターンを指でなぞってロック解除するように設定します。
- ロック No.…ロック No.でロック解除するように設定します。4 桁以上の数字を入力します。
- パスワード…パスワードでロック解除するように設定します。4 文字以上の英数字を入力します。パスワードには英字が 1 文字以上必要です。

3.1.6. VPN 画面で「VPN ネットワークの追加」

「VPN ネットワークの追加」をタップし、VPN ネットワークの編集ポップアップ画面を表示します。



3.2. VPN の設定

3.2.1. VPN ネットワークの編集

VPN の接続に必要な情報を設定してください。



接続名に任意の VPN 名を入力して、「タイプ」（接続方式）を選択してから表示される項目について設定してください。

- 選択した「タイプ」によって設定する項目が異なります。設定する項目の詳細は、「表 1 タイプと設定項目」を参照してください。
- 証明書の指定が必要な場合は、事前にインポートが必要です。証明書のインポートについては、「3.3 証明書のインポート」を参照してください。

表 1 タイプと設定項目

（〇：入力必須、△：条件により入力、－：入力項目なし）

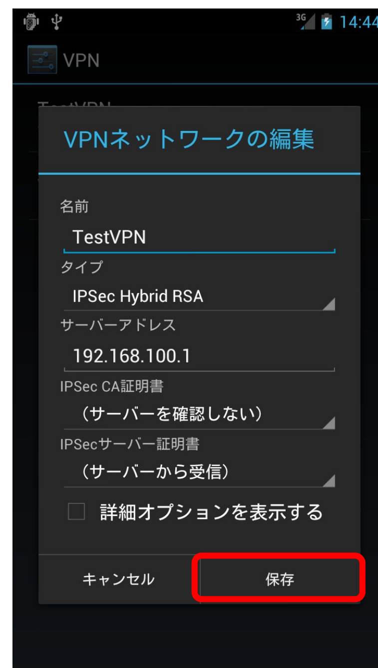
設定項目名	説明	タイプ					
		PPTP	L2TP/IPsec PSK	L2TP/IPsec RSA	IPsec Xauth PSK	IPsec Xauth RSA	IPsec Hybrid RSA
名前	任意の文字列（日本語、英数字）を入力	〇	〇	〇	〇	〇	〇
タイプ	接続環境に応じた接続方式を入力	〇	〇	〇	〇	〇	〇
サーバーアドレス	VPN サーバーのアドレスを入力	〇	〇	〇	〇	〇	〇
PPP 暗号化（MPPE）	PPP 暗号化の有無をチェック	△	－	－	－	－	－
L2TP セキュリティ保護	L2TP セキュリティ保護を入力	－	△	△	－	－	－
IPSec ID	IPSec の ID を入力	－	〇	－	〇	－	－
IPSec 事前共有鍵	IPSec 暗号化用事前共有鍵を入力	－	〇	－	〇	－	－
IPsec ユーザー証明書	ユーザー証明書を選択	－	－	〇	－	〇	－
IPsecCA 証明書	CA 証明書を選択	－	－	△	－	△	△
IPsec サーバー証明書	サーバー証明書を選択	－	－	△	－	△	△
DNS 検索ドメイン 注1)	DNS 検索ドメインを入力	△	△	△	△	△	△
DNS サーバー 注1)	DNS サーバーを入力	△	△	△	△	△	△
転送ルート 注2)	転送ルートを入力	△	△	△	△	△	△

注1）　詳細オプション。DNS を使用する場合に設定する。

注2）　詳細オプション。設定しない場合は、すべての通信が VPN 接続を経由する。設定した場合は、設定したサブネットアドレス宛の通信のみ VPN 接続を経由し、設定されていないサブネットアドレス宛の通信は VPN 接続を経由しない。入力は“ ネットワークアドレス ”/“ サブネットマスク ”の形式で記載する（例：192.168.10.0 / 24)。

3.2.2. VPN ネットワークの編集画面で「保存」

「保存」をタップすると、設定内容が保存され、接続一覧画面が表示されます。
「保存」がグレーアウトされている場合、設定に漏れがないか、入力内容が正しいかをご確認ください。





接続一覧画面に設定した VPN 名が追加されていることを確認してください。
VPN ネットワークは複数作成することができます。
接続、切断の手順は「4 VPN の接続と切断」を参照してください。

保存した設定内容を編集または削除する場合は、接続一覧画面に表示されている「VPN 名」をロングタッチし、表示されるメニューから「ネットワークの編集」または「ネットワークを削除」を選択してください。



3.3. 証明書のインポート

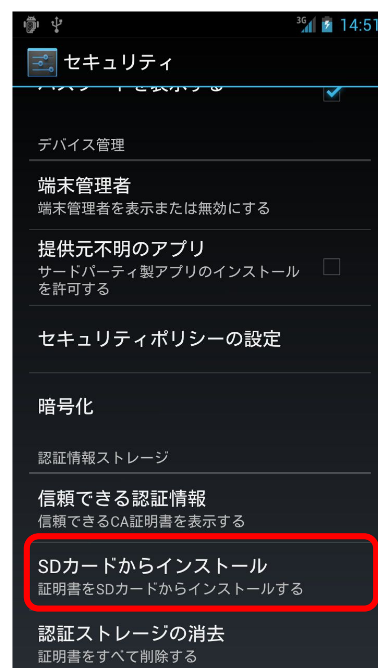
3.3.1. 設定画面で「セキュリティ」

「セキュリティ」をタップし、セキュリティ画面を表示します。



3.3.2. セキュリティ画面で「SD カードからのインストール」

証明書のインポートを行うには、microSD カードのルートディレクトリにインポートする証明書を保存して microSD カードを端末本体に取り付ける必要があります。証明書が保存されている microSD カードが正しく取り付けられていることを確認の上、「SD カードからのインストール」をタップし、次画面を表示します。
microSD カードの取り付けかたについては、端末本体の取扱説明書を参照してください。

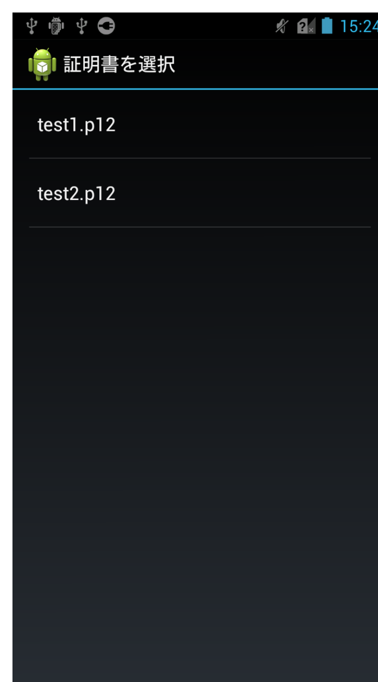


なお、サポートしている証明書は下記です。

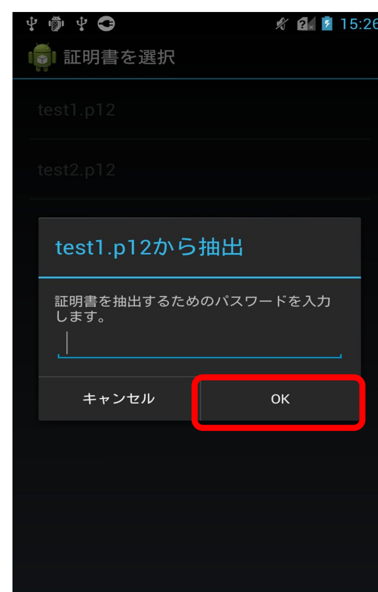
フォーマット	ファイル拡張子
X.509 DER 形式	「.crt」または「.cer」
PKCS#12 形式	「.p12」または「.pfx」

3.3.3. 「証明書を選択」画面で任意の証明書を選択

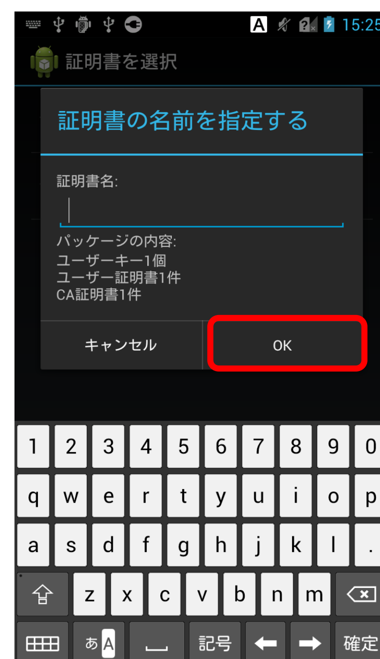
microSD カードに保存した証明書が表示されますので、使用する証明書を選択し、証明書の抽出のためのパスワード入力を行ってください。
ただし、対象となる証明書が microSD カードに１つしかない場合は証明書の選択画面は省略され、証明書の抽出のためのパスワード入力画面が表示されます。



パスワード入力後、OK をタップします。



証明書の名前を指定する画面が表示されますので証明書名を入力後、OK をタップします。

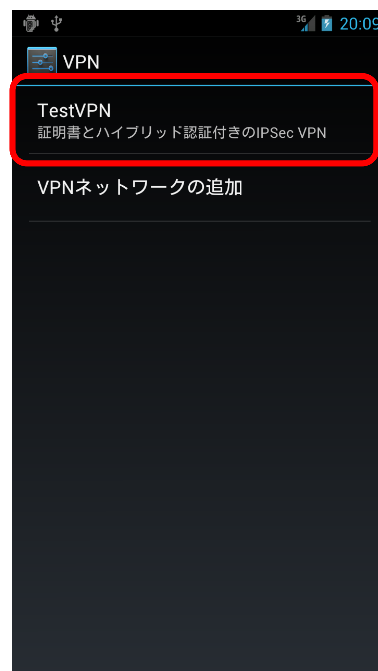


4. VPN の接続と切断

4.1. VPN の接続

4.1.1. 接続一覧画面で接続する「VPN 名」を選択

「VPN 名」をタップすると、ユーザー名、パスワードを入力するポップアップ画面が表示されます。



ユーザー名、パスワードをそれぞれタップし、入力してください。

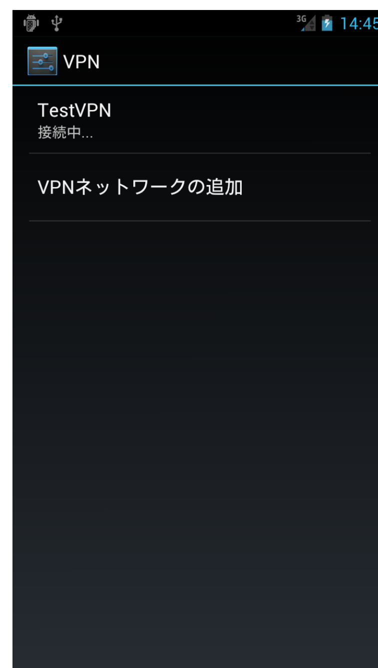


4.1.2. 「接続」を選択

必要な情報を入力後、接続をタップします。
なお、接続前に「アカウント情報を保存する」をチェックすると、次回より、ユーザー名の入力が省略可能となります。



接続中は、「VPN 名」の下に「接続中」と表示されます。



VPN サーバーに接続されると、「VPN 名」の下に「接続されました」と表示され、画面上部に のアイコンが表示されます。



4.2. VPN の切断

4.2.1. 通知パネルを開き、VPN の通知を選択

「VPN が有効化されました。」と表示されている通知をタップすると、VPN 接続済みのポップアップ画面が表示されます。



4.2.2. VPN 接続ポップアップ画面で「切断」

「切断」をタップすると VPN サーバーと切断されます。



5. 商標について

- 「FOMA」は NTT ドコモの商標または登録商標です。
- 「MEDIAS」は NEC カシオモバイルコミュニケーションズ株式会社の商標または登録商標です。